

Simplifying Cyber Security since 2016

HACKERCOOL

October 2024 Edition 7 Issue 10 Learn how Black Hat Hackers hack

Hacking Active Directory

BLACK HAT HACKING

How Watering Hole attack works and how to stay safe from this attack.

WHAT's NEW

Parrot Security 6.2

VULNERABILITY FOR BEGINNERS

Mozilla Firefox CVE-2024-9680



Copyright © 2024 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 7 Issue 10

8 years passed just like that. Yes, it's been 8 years since we started Hackercool Magazine. Just like last year, this year too saw lot of developments in Hackercool Magazine and the office where it is made. However, just like kernel and package updates we have been seeing a lot in latest releases of penetration testing distros recently, many changes and updates that happened at Hackercool Magazine happened on backend. So, you may not even notice them or they even catch your attention.

However, there are a few updates and new things that you may notice and even raise your head to get a better look. When you read this Issue, you will see that the article feature "Active Directory" is back. It's first appearances ended with a whimper but we have better plans for this feature aptly named "Rebirth".

With 8 out of 10 hacking attacks observed in real-world making Windows Active Directory their target, any Hacker Magazine that does not have this feature is not a hacker magazine. In its previous outing, it was backend that brought down this feature and we have better prepared the same backend now (or maybe we think so). With this feature, we want to bring you all the hacking attacks that happen in Active Directory in real-world. Keep watching this feature for more.

There is another change we made which you will notice only while buying or in some cases renewing our subscription plans or bundles. It is that we have added new payment methods to checkout for our customers. There has been complaint our would-be customers have been making since a long time. That the checkout currency is only in US Dollars.

We have added support to multiple currencies enabling customers to pay with their local currency. Now you can pay with currency of your choice, since we have added support to EUR, GBP, CAD, AUD and many more currencies. Just go to our product page and check if your preferred currency is available or not.

We have also added new payment methods. Earlier, we just used to have PayPal checkout. Now we have added another payment method Cashfree payment gateway. This enables us to accept payments from our Indian users along with international customers around the world. You can also pay with Cashfree using any international card you like.

You should have already received a mail regarding this with detailed explanation. For our Indian users we have enabled PhonePe payments. We will be adding more payment methods for our Indian users soon.

Apart from Cashfree, we have enabled WIRE TRANSFER payment method again. This year we have been going around the globe (not in the physical realm) for creating Local Bank accounts in our company's name. As by now, we have local Bank accounts in USA, UK, European Union, Australia, Canada, and Singapore in the name of our company. Customers in these countries can just use local payment methods to pay or transfer money to these accounts.

If you are not from any of the above-mentioned countries, don't get disappointed. We have also created a universal account to accept money from you. Please use whichever payment method is comfortable to you. Your payment, your choice.

There are all the changes that took place at Hackercool Magazine. There are many other changes too but I already said these are backend changes and you may not notice them.

INSIDE

See what our Hackercool Magazine's October 2024 Issue has in store for you.

1. Black Hat Hacking:

Watering Hole Attack explained.

2. Vulnerability for beginners:

Mozilla Firefox 's CVE-2024-9680 zero-day vulnerability.

3. What's New:

Parrot Security OS 6.2

4. Cyber Security:

Is your car a threat to national security? It can be - regardless of where it's made.

5. Hacking Active Directory:

Rebirth

6. Vulnerability for beginners:

TrendMicro Cloud Edge CVE-2024-48904 vulnerability.

7. Online Security:

As an ethical hacker, I can't believe the risks people routinely take when they access the internet in public.

8. Exploit Writing:

Converting Python scripts to Binaries.

Downloads

Other Useful Resources

Watering Hole Attack

BLACK HAT HACKING

Dogoo jee (name changed) was viewing a website. He was living in Australia and just like a number of Tibetan Buddhists around the world, he was excited about the Kagyu Monlam festival to be held from December 15 to 21, 2023. The festival is held every year at Bodhi Gaya, India and it attracts thousands of Buddhists who gather to pray for peace, listen to teachings and perform other activities. The festival is led by the Holy Lamas of Tibetan Buddhism.

Dogoo jee wanted to know more about the Kagyu Monlam as he wanted to visit it that year. So, he opened the website of Kagyu Monlam International Trust, an organization based in India that promotes Tibetan Buddhism internationally.

As he was browsing through the website, he got an error page asking him to download a 'fix' named "certificate.exe" to fix that error. Dogoo jee downloaded and installed the fix to fix that error on the website. In Jan 2024, ESET researchers detected that this website was a target of a cyber espionage campaign and identified the threat actor as Evasive Panda also known as Bronze Highlander and Daggerfly. Little did he know that Dogoo jee activated a downloader that would start a long infection chain to compromise his system.

As you might have guessed by now, the website was made a target for watering hole attack by a Chinese threat actor.

Introduction

In Black Hat Hacking feature of this month's Issue, you will learn what is a watering hole attack, how is it performed, how it can be exploited, its impact and how to protect oneself from these types of attacks.

What is watering Hole attack?

In Cyber security, watering hole is an attack in which the hacker compromises a website that is frequently visited by users of an organization to gain initial access to the organization's network. The name watering hole came from the same strategy used by predators in the forests. Instead of chasing prey, they lay an ambush at the watering hole because wherever prey go, they will definitely return to drink water.

In December 2012, in what is supposed to be a watering hole attack, the website belonging to the Council on Foreign Relations of USA was found to be infected with malware through a zero-day vulnerability in Microsoft's Internet Explorer.



In Cybersecurity, the same strategy is used. Instead of targeting an organization's defenses, the hacker compromises a website which is frequently visited by users of an organization and a malware is served from this website. Watering hole attack is also known as strategic web compromise.

In a watering hole attack, apart from the website the TRUST of the users is exploited. This is because people rarely presume popular and most visited websites will be compromised.

Watering Hole Attack

How the attack is performed?

Just like any hacking attack, watering hole attack too requires a number of steps. This attack start

s by gathering as much information about the target user in order to profile them.

How Watering Hole attack works?



STEP 1:

A hacker profiles his intended target users to find out the websites they visit most.

Hackercool Magazine



STEP 3:

The unsuspecting user visits this website and is infected.



STEP 2:

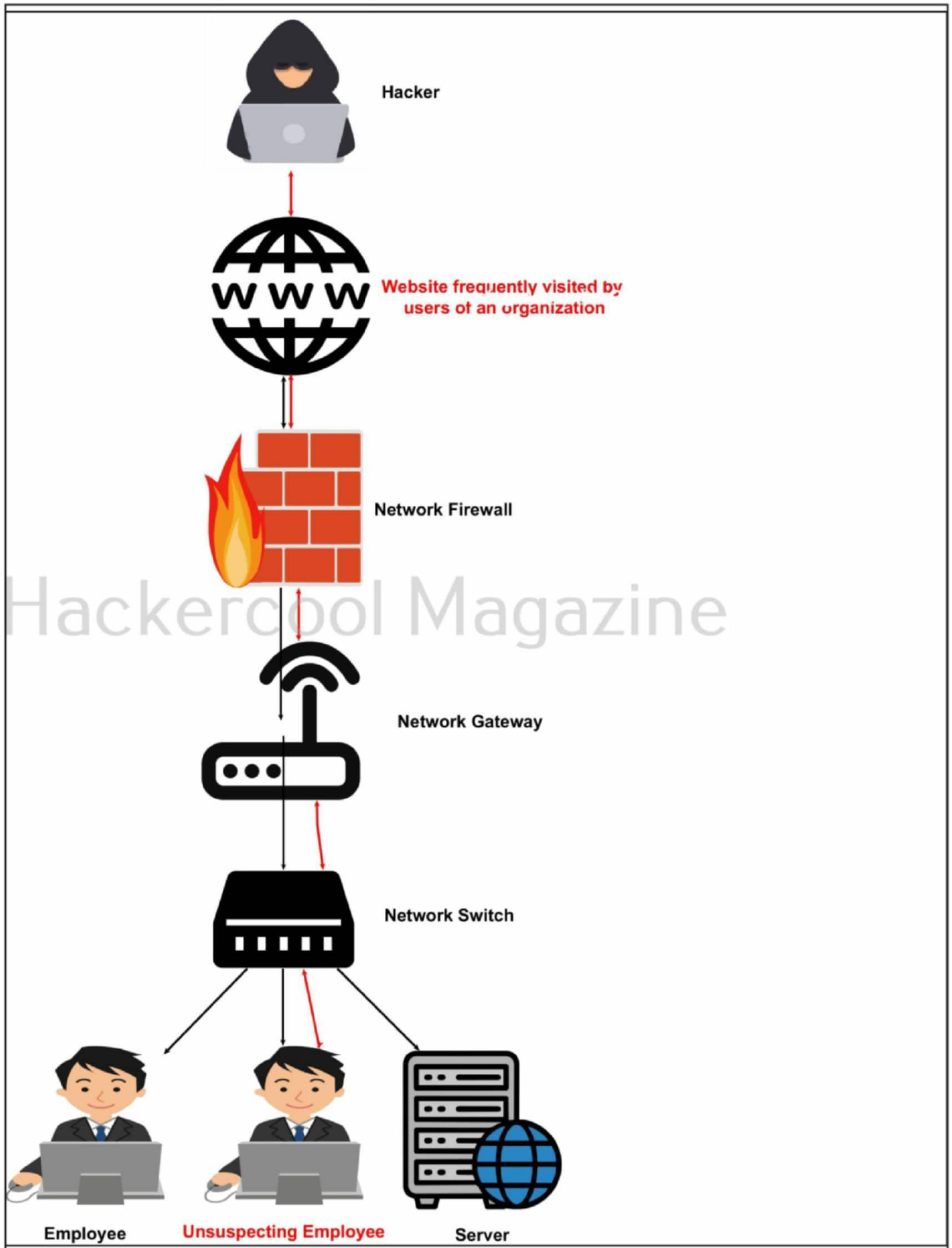
The hacker compromises the security of this website and changes its code to plant customised payload.

In the example given at the beginning of this article, Evasive Panda, a Chinese threat actor known to target Tibetan exile community, targeted users visiting to that particular website from locations like India, Taiwan, Hong Kong, Australia, and United States. Since their target were Tibetan users, they targeted countries with a large Tibetan diaspora. Then, they targeted a website frequently visited by these users.

In the next stage, they exploited this website and gained access to it. Then they added a script to this website that showed a fake error page to users with IP addresses from the above countries. Then they placed a malware on the website. This malware or payload is most probably a custom payload. This website can be compromised using any means like exploiting a zero-day vulnerability etc. They then installed a script that would show an error page to users visiting from the above-mentioned locations. That too at the time nearing Kagyu Monlam festival. They knew many Tibetans would definitely show lot of interest in Kagyu Monlam festival. (Apart from this website, hackers compromised two other websites frequented by Tibetans and added the above-mentioned code).

Next step is to make the user download the payload and execute the payload.

In 2015, the U.S. government seized a Tor (network) website and installed a malware based "Network Investigative Technique" (NIT) on this website. This malware allowed them to hack into the web browsers of users accessing the site, thereby revealing their identities. This operation led to the arrest of over 956 website users of Playpen, a darknet child pornography website.



Impact

Watering hole attack is very rarely used but its effectiveness is very high. This is the exact reason why many Black Hat Hacker groups continuously use it even now. Depending on the payload and the hacking group's goal, hackers can do anything once he gains initial access on the target network. This can lead to ransomware attack, data breaches etc.

How to protect yourself from this attack?

A Watering Hole attack is difficult to detect, as hacking activity is not occurring on the network of your organization but outside your network.

But some measures can help you protect your network from watering hole attack.

1) **Web Gateway:** A web gateway is a security Solution that monitors and controls what websites are being visited, what files are being downloaded and protects you from unexpected drive-by downloads.

2) **EDR:** Most of the watering hole attacks use custom malware or payloads, so using a robust EDR can detect its malicious activity.

3) **Regular security testing:** Regularly testing your network for any security threat or malicious actions can protect you from these types of attacks.

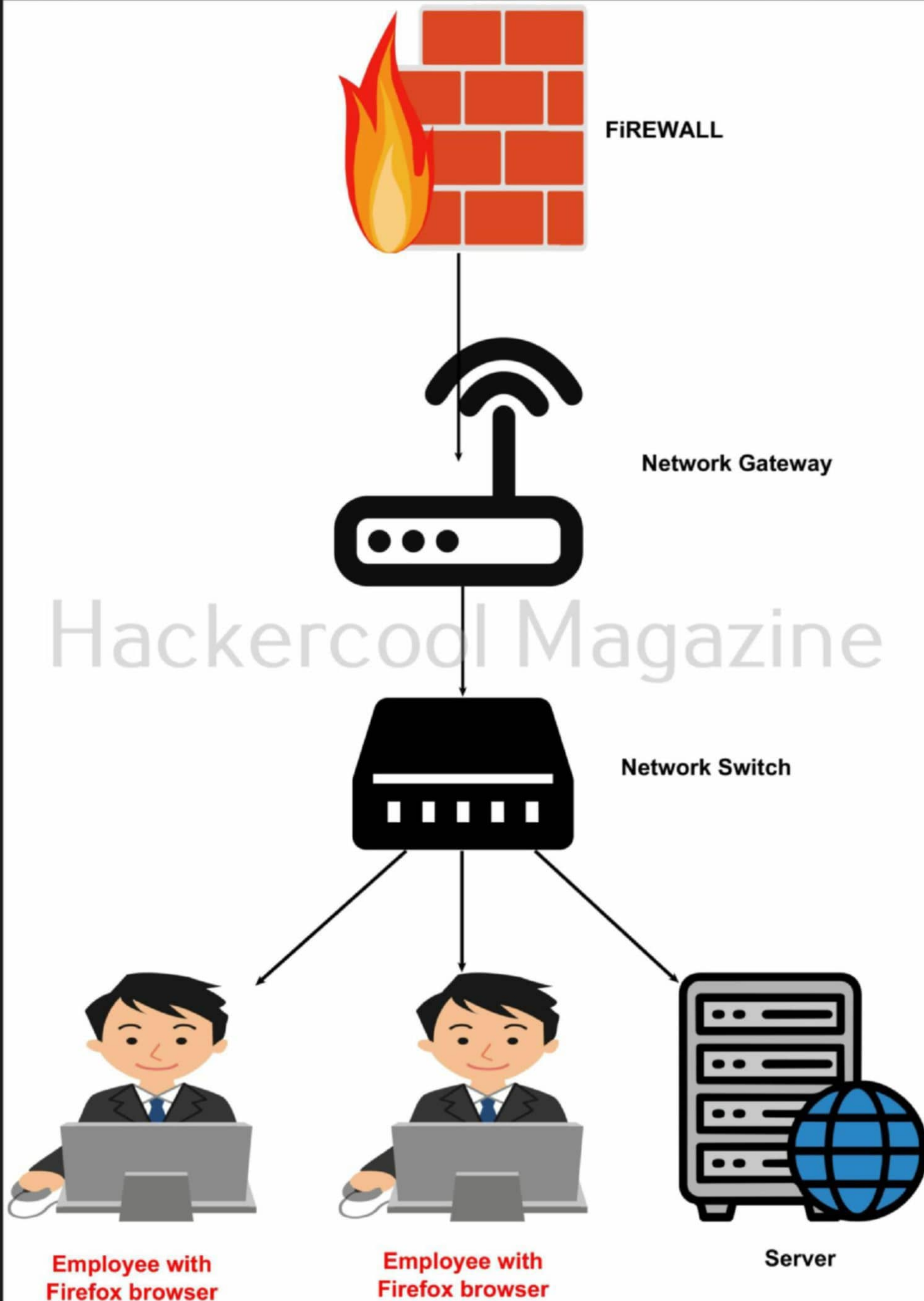
4) **Suspect all the traffic:** We usually think some of the popular websites are safe but you have to treat all the traffic as suspicious in order to maintain the security of the organization.

Mozilla Firefox CVE-2024-9680

VULNERABILITY FOR BEGINNERS



Mozilla Firefox is one of the widely used browsers around the world. It is used by over 178 million people around the world. An RCE vulnerability in browsers is being exploited in the wild.



The vulnerability, being tracked as CVE-2024-9680, has a severity of 9.8 out of 10 in CVSS rating. It also doesn't require much complex action to exploit this vulnerability.

The vulnerability is a use after free vulnerability in the animation timeline component of the browser. Animation timelines are a mechanism of Firefox web animation API and are used to control and synchronize animations on web pages. The credit for discovering this vulnerability goes to security researcher Damien Schaffer from Slovakian cybersecurity company ESET.



The use-after-free vulnerability occurs when a memory that has been freed is still used by the program. This allows hackers to add their own malicious commands to the memory and then perform code execution. This vulnerability affects version 131.0.2 Firefox ESR 128.71 and Firefox ESR 115.16.1. The same vulnerability also affects Tor Browser and this also is being exploited in the wild. By exploiting this vulnerability, the hacker can take control of Tor Browser.

How can this vulnerability be exploited?

This vulnerability can be exploited remotely to execute code and doesn't even need user interaction. Although the method of how this vulnerability is being exploited in the wild is not known, it can be weaponized either by a watering hole attack or a drive-by download attack.

Impact

The impact of this vulnerability can be dangerous as any remote code execution vulnerability.

Depending on the situation it can be further used to data breach, ransomware attack etc.

How to prevent its exploitation?

Within 24 hours of the disclosure of the vulnerability Mozilla has released the patch for this vulnerability. However, the release of the patch itself is not going to fix this vulnerability. You have to update your browsers to the latest version. The version of Mozilla Firefox safe from this vulnerability are Firefox 131.0.2 and Firefox ESR 115.16.1 or 128.3.1. Tor Browser version should be 13.5.7. You can update your browser by going to Tools menu >Help>About Firefox. The browser will update automatically.

Parrot Security OS 6.2

WHAT'S NEW

Parrot Security OS, popularly called as Parrot OS, is a penetration testing operating system that differs from other hacking operating systems by focusing more on privacy apart from pen testing. The makers of Parrot OS have released the latest version of their operating system, Parrot Security OS 6.2. Let's see what new features they have added to it.



One of the most common ways cyber criminals get access to your data is through your employees. They'll send fraudulent emails impersonating someone in your organisation and will either ask for personal details or for access to certain files. Links often seem legitimate to an untrained eye and it's easy to fall into the trap. This is why employee awareness is vital.



Latest Features to be excited about.

Updated tools

As I always say, what is a new release of an ethical hacking distro that either doesn't add a new tool or updates to new tools. Just like this, in the latest release of Parrot Security OS, many tools were updated. Airgeddon was updated to its latest version 11.30.

"Keep your software and systems fully up to date"

Often cyber attacks happen because your systems or software aren't fully up to date, leaving weaknesses. So cybercriminals exploit these weaknesses to gain access to your network. Once they are in – it's often too late to take preventative action.

To counteract this, it's smart to invest in a patch management system that will manage all software and system updates, keeping your system resilient and up to date.


```

***** Welcome *****
*****

This script is only for educational purposes. Be good boyz&girlz!
Use it only on your own networks!!

Accepted bash version (5.2.15(1)-release). Minimum required version: 4.2

airgeddon needs root permissions to work. Launch the script as root user c
r using "sudo"

***** Exiting *****
*****

Exiting airgeddon script v11.30 - See you soon! :)

Checking if cleaning/restoring tasks are needed...
Cleaning temp files .... Ok

```

The latest version of airgeddon adds support to launch more than one airgeddon instance at a time, improves some 5GHz band capability detection and fixes some bugs. Another tool to get updated is Anonsurf.

```

[~]-[user@parrot]-[~]
$anonsurf
AnonSurf [5.0.0] - Command Line Interface

Developed by:
  Lorenzo "Palinuro" Faletra <palinuro@parrotsec.org>
  Lisetta "Sheireen" Ferrero <sheireen@parrotsec.org>
  Francesco "Mibofra" Bonanno <mibofra@parrotsec.org>
Extended by:
  Daniel "Sawyer" Garcia <dagaba13@gmail.com>
Maintained by:
  Nong Hoang "DmKnight" Tu <dmknight@parrotsec.org>
and a huge amount of Caffeine, Mountain Dew + some GNU/GPL v3 stuff

Usage: anonsurf <options>

```

DeepMagic information gathering tool (Dmitry) is another tool that is updated to its latest version.

In the event of a disaster (often a cyber attack) you must have your data backed up to avoid serious downtime, loss of data and serious financial loss.


```
[*]-[user@parrot]-[~]
```

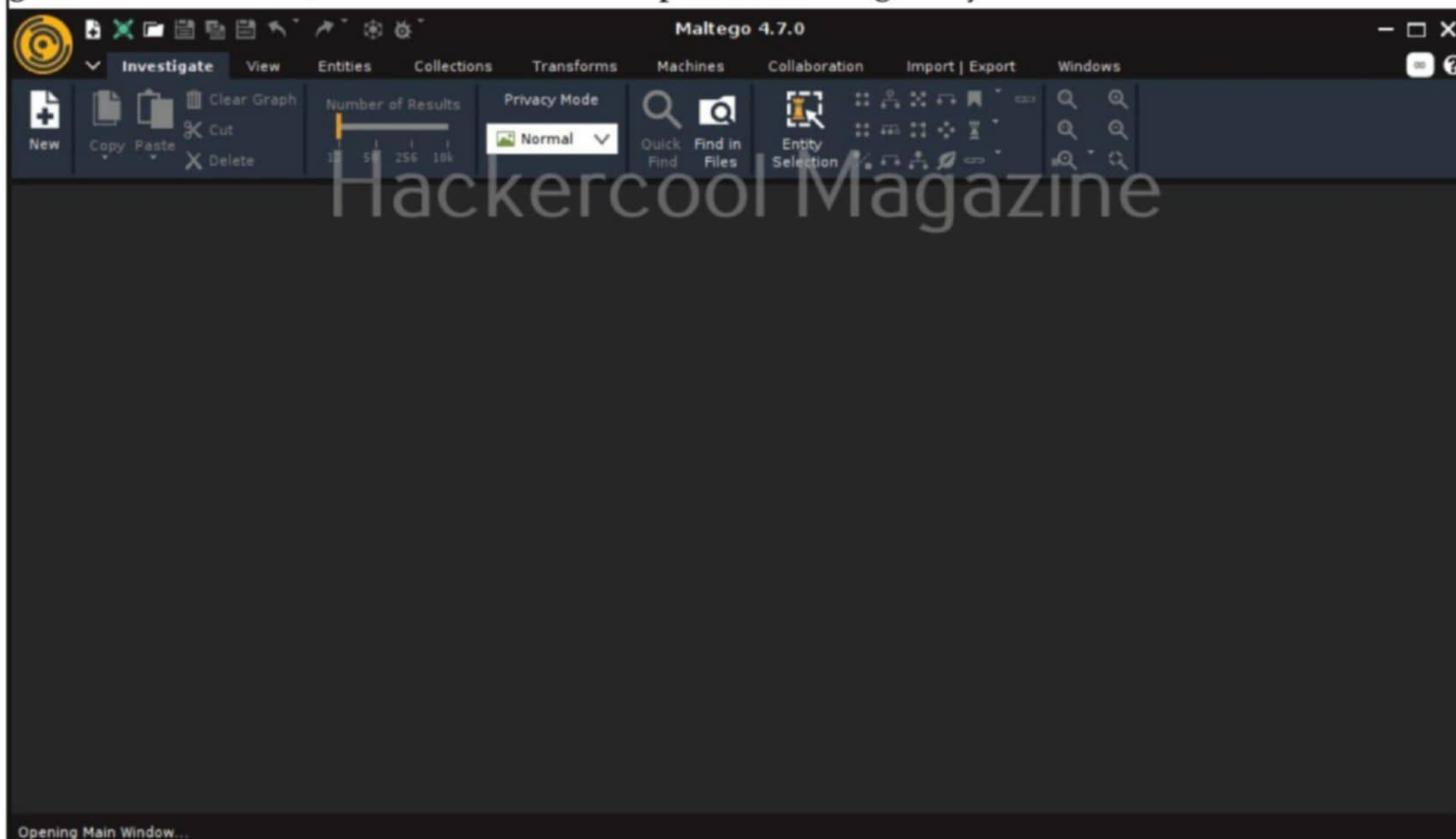
```
$dmitry -v
```

Deepmagic Information Gathering Tool

"There be some deep magic going on"

Version: DMitry/1.3a (Unix)

This latest version of the tool fixes two major issues with mailsearch and subsearch. Maltego, another information gathering tool too got updated to version 4.70. This version adds a new graph recovery option to the tool. It also adds enhanced user prompt capabilities, user onboarding with a guided in-client tour, new data sources etc apart from fixing many issues..



NetExec tool has been updated to version 1.2.0.

```
[*]-[user@parrot]-[~]
```

```
$netexec --version
```

1.2.0 - ItsAlwaysDNS

```
[*]-[user@parrot]-[~]
```

```
$
```

This release of NetExec adds so many network features like dumping SCCM credentials, looting of PuTTY credentials and RSA Private keys, new LDAP flags for retrieving active users on the Domain, a new LDAP module, new WinLogon Autologon module etc.

Apart from the above tools, many other tools and packages have been upgraded to the latest version. They are Bind 9, Chromium Codium, Flatpak, Libre Office and VLC etc. Thanks to the latest vulnerability, you studied above, Firefox and Tor have also been updated to its latest version.


```
[x]-[user@parrot]-[~]
$firefox --version
Mozilla Firefox 131.0.3

[user@parrot]-[~]
$tor --version
Tor version 0.4.8.12.
This build of Tor is covered by the GNU General Public License (https://www.gnu.org/licenses/gpl-3.0.en.html)
Tor is running on Linux with Libevent 2.1.12-stable, OpenSSL 3.0.14, Zlib 1.2.13, Liblzma 5.4.1, Libzstd 1.5.4 and Glibc 2.36 as libc.
Tor compiled with GCC version 12.2.0

[user@parrot]-[~]
$
```

Rocket Tool

Another feature to be excited about in the latest release of Parrot OS is a new tool named Rocket. Rocket is a launcher for launching Docker containers. Entirely written in Python using PyQt6 for GUI, it can be very useful in launching the many security tools from Docker repositories, especially from Parrot OS Docker repository. It obviously requires installation of Docker. Its download information is given in our Downloads section.

Once downloaded, the archive can be extracted to reveal a .deb file. This deb file can be installed as shown below.

```
[user1@parrot]-[~/Desktop]
$sudo dpkg -i rocket_1.2.0-1_amd64.deb
(Reading database ... 540499 files and directories currently installed.)
Preparing to unpack rocket_1.2.0-1_amd64.deb ...
Unpacking rocket (1.2.0-1) over (1.2.0-1) ...
Setting up rocket (1.2.0-1) ...
```

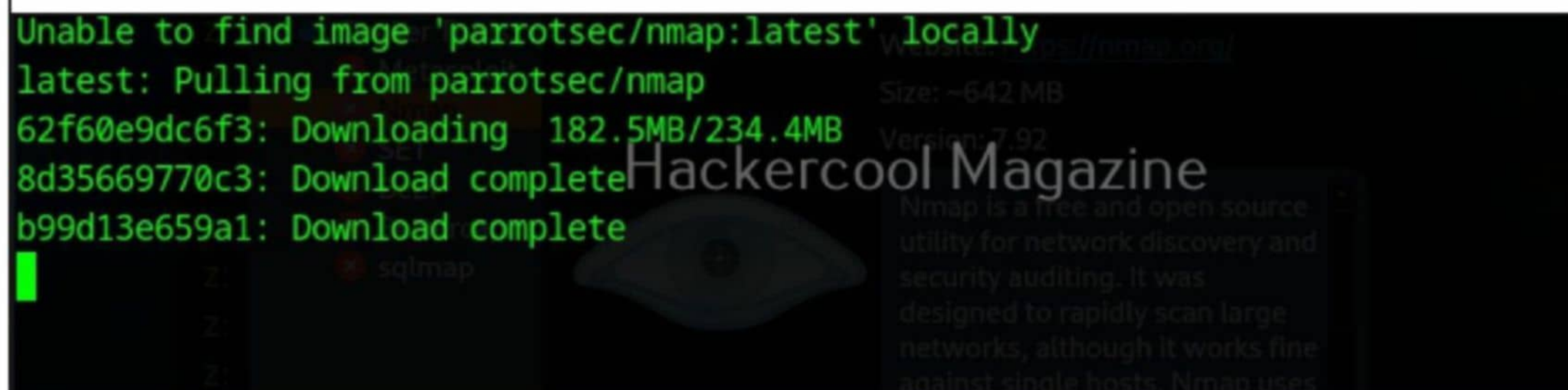
It is installed in the /usr/bin/ directory and has to be started from there.

```
[user1@parrot]-[/usr/bin]
$ /usr/bin/rocket_1.2.0
```

There are so many different types of sophisticated data breaches and new ones surface every day and even make comebacks. Putting your network behind a firewall is one of the most effective ways to defend yourself from any cyber attack. A firewall system will block any brute force attacks made on your network and/or systems before it can do any damage, something we can help you with.



Any docker container can be started by selecting and clicking on “Run container”. This will download the relevant docker image. For example, let’s select Nmap and click on “Run container”. This will result in this.



Every employee needs their own login for every application and program. Several users connecting under the same credentials can put your business at risk. Having separate logins for each staff member will help you reduce the number of attack fronts. Users only log in once each day and will only use their own set of logins. Greater security isn’t the only benefit, you’ll also get improved usability.

Parrot Terminal

Edit View Search Terminal Help

Rocket

Docker Tools

- Metasploit
- Nmap
- SET
- BeEF
- Bettercap
- sqlmap

Website: <https://trustedsec.com/resources/tools/the-social-engineer-toolkit-set>

Size: ~2.43 GB

Version: 8.0.3

The Social-Engineer Toolkit is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack quickly. SET is a product of TrustedSec, LLC – an information security

CLI usage examples

```
setoolkit
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Website Attack Vectors
```

Run Container Stop Container

Info Docker is running

Other important updates added

The Linux Kernel has also been updated to 6.10.11. This adds support to AMD and Intel processors.

```
[user1@parrot]-[~]
$uname -v
#1 SMP PREEMPT_DYNAMIC Debian 6.10.11-1parrot1 (2024-10-03)
[user1@parrot]-[~]
$
```

Other features added

The kernel for raspberry pi has also been updated. These are the features added to the latest release. Which one among this you will find more helpful?

Having managed admin rights and blocking your staff installing or even accessing certain data on your network is beneficial to your security. It's your business, protect it!

Is your car a threat to national security? It can be – regardless of where it is made.

CYBER SECURITY

Dennis B. Desmond

Lecturer, Cyberintelligence and Cybercrime Investigations, University of the Sunshine Coast

In April, US lawmakers urged President Joe Biden to ban Chinese-built electric vehicles (EVs), labelling them an “existential threat to the American auto industry”. The proposed ban arose from concerns that Chinese car makers have an unfair advantage due to government financial support.

Following a months-long investigation into digital connections that could enable Chinese spying and sabotage, in recent weeks the Biden administration proposed new rules to ban Chinese-made vehicles. The threats they cite stem from built-in internet connectivity for software updates and various remote controls.

Is the US justified in aiming to ban Chinese-made cars over national security issues, and should Australia follow suit? Remote access and data transmission are an integral part of Chinese cars, but the same is true of modern cars made in most countries.

However, Australia’s relationship with Beijing has been rocky at times. Therefore, it’s vital to understand what data is being sent to China and how any vehicles sold in Australia are vulnerable to remote access and control.

Convenience as a double-edged sword

Many car makers offer remote services, including control over vehicle functions. These features are convenient, but also raise concerns about control, privacy and security.

Modern cars are like computers on wheels. They collect data about the car and the driver which can be accessed remotely or during servicing. Computerised control systems and monitoring (also known as telematics) have become widespread.

Regardless of whether the car is electric or petrol-fuelled, the concern is who has access to all that data, and how. If it’s not sent over the internet, but simply downloaded and analysed at the local garage, that’s arguably less concerning.

OnStar, a subsidiary of General Motors launched in 1996, pioneered vehicle telematics and remote connectivity. US law enforcement and intelligence agencies have previously used OnStar’s services to track vehicles, listen to in-car conversations, and even to slow down vehicles during pursuits.

It’s now common for car makers to deliver updates, new features and performance improvements remotely. Volkswagen’s connected service app includes remote start, door lock, vehicle status checks, roadside assistance, vehicle health reports and service scheduling.

Similar apps exist for Ford, Mazda and BMW cars, among others. Earlier this year, police alleged

"Privacy concerns over internet-connected cars have been widely reported before. But the latest commentary goes beyond this, implying national security risks. Due to so much connectivity, it's possible for hackers or even nation-states to attack connected vehicles."

(Cont'd On Next Page)

-edly used an app tracking feature to retrieve a stolen Ford Ranger in Melbourne.

Haval and GWM, two Chinese car manufacturers, also offer connected services for their electric and petrol vehicles in Australia. In some GWM cars, "T-Box" telematics hardware allows the car to connect to the internet. If activated through the manufacturer's app, GWM ConnectService collects temperature, battery status, estimated range, mileage, tyre pressure and location. It can also remotely control locks, headlights and other features.

Privacy concerns over internet-connected cars have been widely reported before. But the latest commentary goes beyond this, implying national security risks. Due to so much connectivity, it's possible for hackers or even nation-states to attack connected vehicles.

Last week, Coalition member Barnaby Joyce expressed concerns China could weaponise remote access to its EVs for "malevolent purposes". This worry stems from the fact that in Australia, more than 80% of EVs sold are manufactured in China (this includes Tesla models).

Between reality and science fiction

Security experts have raised concerns about China being able to collect driver geolocation and behavioural data, especially in military settings. In the US, car-based espionage concerns have prompted investigations into foreign-made car hardware and software.

To find out whether Chinese cars have actually been used in espionage, governments will need to engage in further scrutiny. This should include increased counterintelligence measures.

Another concern is the remote disabling of vehicles. It is possible to remotely disable a car. Ford filed a patent for remote disabling of services in 2023. Some GWM models currently have built-in alarms and immobilisers that disable a car if unauthorised use is detected.

Moreover, some car manufacturers offer post-theft tracking services, allowing for remote immobilisation. A car equipped with these features could theoretically be hacked by a malicious actor.

Recently, Chechen leader Ramzan Kadyrov accused Elon Musk of disabling his Tesla Cybertruck in Ukraine, where Kadyrov is supporting Russia's military actions.

This unverified incident hints that a foreign entity could target vehicles over which they have control. However, the possibility of China disabling cars during a trade dispute, cyber conflict or conventional war seems like something out of dystopian fiction.

Who has access to the data?

"Recently, Chechen leader Ramzan Kadyrov accused Elon Musk of disabling his Tesla Cybertruck in Ukraine, where Kadyrov is supporting Russia's military actions."

Ultimately, the worry that nation-states can use highly invasive bits of tech in our cars for spying is not entirely unwarranted.

When you buy a modern car with built-in computers and connected services, you agree that car use data and personal information can be shared with garages and manufacturers. But when we purchase an item, we expect to own it and have full control over its use.

If you're worried about privacy, take charge. Your best recourse is to know what information your car is collecting, with whom the manufacturer is sharing that information, and where and how that information is being stored and used.

**This Article
first
appeared
in
The Conversation**

HACKING ACTIVE DIRECTORY

According to Semperis, the company specializing in Active Directory (AD) Security, ransomware risk report 2024, 9 out of 10 hacking attacks target Active Directory. Out of these 9 attacks, over 87% of them completely disrupt the operations of an organization causing data loss and downtime. This should be enough to give you an idea about how important Active Directory security is. In the first article of this feature, you will learn in detail what Active Directory is, how is it useful and why many organizations use it etc.

What is Active Directory?

Active Directory is a set of services and a database that connects users of an organization with each other and allows them to share resources of the organization to get the work done. The database is present in one device known as Domain Controller (explained below) which has critical information about all user accounts and their rights in the domain (explained below).

How is it useful?

Let me answer this question with an example. You should have seen that the heading of this feature is called “Rebirth”. Have you ever thought about the reason for naming this article like this. Let me explain. If you are one of our oldest subscribers of Hackercool Magazine you should have realized that this is not the first time we are having a feature on Active Directory hacking. Earlier too we had one, although not with the same name. However, it ended in a whimper. I mean to say I ended it as soon as we started it. One of the reasons for this was I started my magazine on a single Laptop (on which all hacking labs were present) I bought for doing my engineering project. It was an 8GB enabled machine.

Even after increasing the RAM to its maximum capacity of 16 GB, running a Windows Domain Controller, Windows Client (The machine that connects to the Domain Controller) machine and Kali Linux (attacker system). On one Laptop was extreme and frustratingly slow.

Then I had an idea. I bought another Laptop. With two machines working now, I thought of juggling virtual machines on both Laptops. I called this arrangement Moving labs. Although this solution worked for some time, it was still problematic. Hiring another employee meant I had to make one Laptop available to him for Magazine related works and this made labs unavailable for most of the time.

I think we are getting carried away. We will tell you how we solved this problem later. Let’s focus on how Active Directory is useful to organizations.

Active Directory enables centralized management of company’s resources, users and rights management. It also simplifies life of administrators while ensuring security of an organization. Let me explain with an example.

Imagine a company with 4 employees. These 4 employees have different roles in completing a project. They work on a Windows Workgroup environment as the company is still small.

“Information is power. But like all power, there are those who want to keep it for themselves.”

Computer Name/Domain Changes



You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:

DESKTOP-FIPSAV7

Full computer name:

DESKTOP-FIPSAV7

More...

Member of

☐ Domain:

☒ Workgroup:

WORKGROUP

OK

Cancel

“We are the voice of the voiceless, the eyes of the blind, the hands of the powerless.” - Anonymous hacker.

Fig: A company with 4 employees.

Hackercool Magazine

**Employee 1****Employee 2****Employee 3****Employee 4**

The company's projects are such that each user has to access some data from three computers from time to time. Earlier these employees (although it's a bit awkward) worked by changing their positions physically from one computer to another computer. They sometimes also shared data using USB drives. But they needed LIVE access most of the time.

Seeing this was not only disturbing other workers but also wasting a lot of time, the company management installed a Remote Desktop Server on each of the 4 computers and created an account for each of the four users on each server.

Fig: A company with 4 employees and 4 RDP servers

Hackercool Magazine

**Employee 1
with 4 RDP accounts****Employee 2
with 4 RDP accounts****Employee 3
with 4 RDP accounts****Employee 4
with 4 RDP accounts**

If you have noticed, earlier there used to be one local user account on each computer but now there are 4 RDP servers in the network each with four user accounts. This made security a bit complex but work improved.

After some time, the number of workers of the company increased to 10. If the company had to still follow the decentralized model they have used above, it will need 10 RDP Servers running on each of the 10 systems, each with 10 user accounts.

"Hacking is very interesting. Once they hack, if you don't catch them in the act, you're not going to catch them."
-Donald Trump

Fig: A company with 10 employees and 10 RDP servers



That would be increasing maintenance of security for the management apart from making it complex. There will be 100 user accounts of RDP on the entire network with each RDP server having 10 user accounts. Apart from all the problems this arrangement brings with it, it will increase chances of security incident.

The only solution is centralization. After much thinking, the management sets up a Windows Server, creates a domain, enables File and Storage Services, Remote Desktop Service on it and creates 10 user accounts for each one of the 10 employees on that server.

Control access to your systems

"Believe it or not, one of the attacks that you can receive on your systems can be physical, having control over who can access your network is really really important.

Somebody can simply walk into your office or enterprise and plug in a USB key containing infected files into one of your computers allowing them access to your entire network or infect it. It's essential to control who has access to your computers. Having a perimeter security system installed is a very good way to stop cybercrime as much as break ins!"

Computer Name/Domain Changes



You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:

DESKTOP-FIPSAV7

Full computer name:

DESKTOP-FIPSAV7

More...

Member of

☒ Domain:

☐ Workgroup:

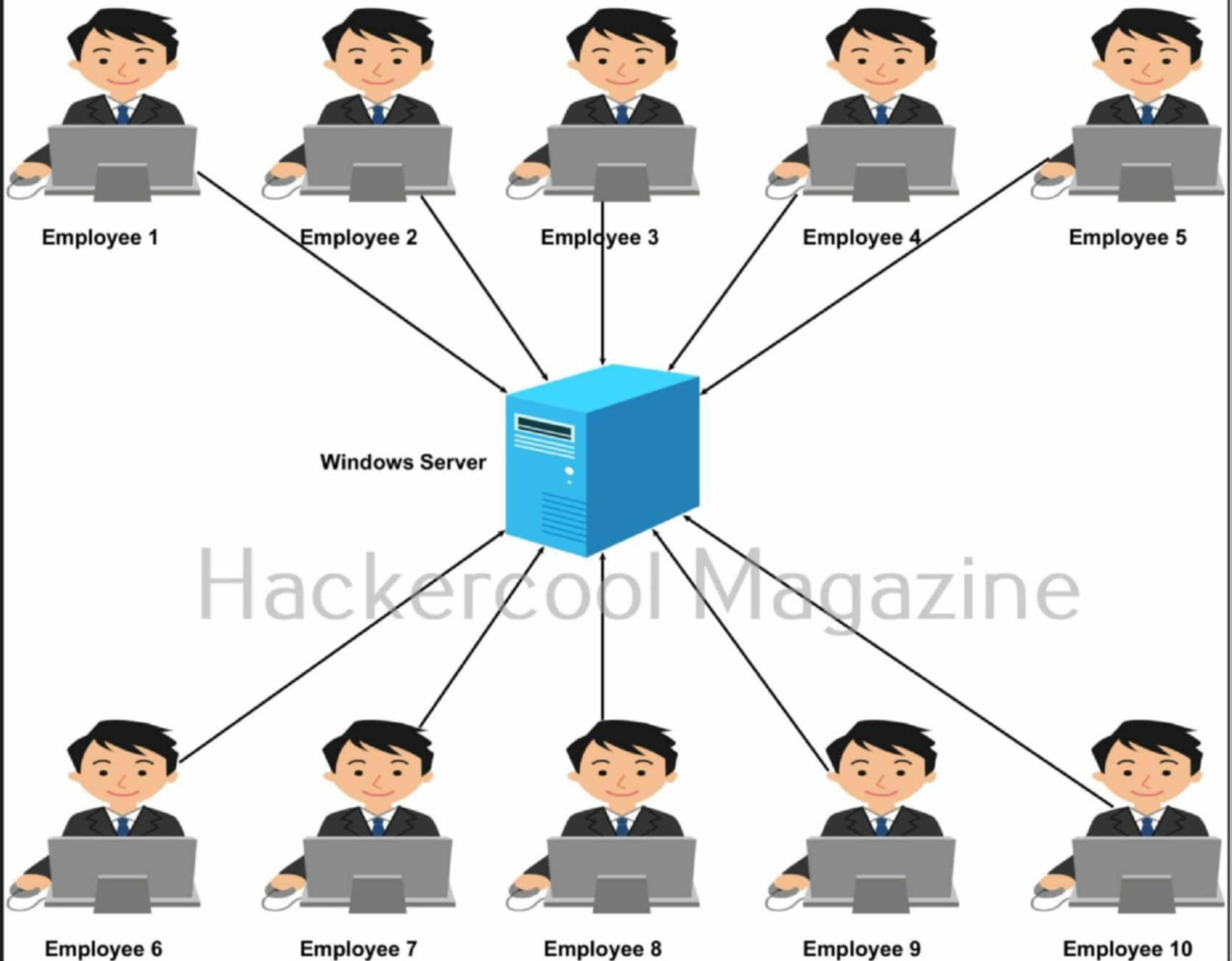
WORKGROUP

OK

Cancel

"You can do reverse engineering, but you can't do reverse hacking."
-Francis Crick

Fig: A company with 10 employees on a domain



Anybody who needs any data can just login into his account on the Windows server and access whatever he needs. Instead each user having 10 RDP user accounts, he/she has just one now. This not only makes it easy for the employees but also from administration of network security. I hope I have been able to convey the use of Active directory properly to you.

Active Directory was first introduced by Microsoft with Windows 2000. The latest version of Windows Server is Windows Server 2022. The roles present in a window Server include,

- 1) Active Directory Domain Service (ADDS)
- 2) Web Server (IIS)
- 3) DHCP Server
- 4) DNS Server
- 5) Hyper-V
- 6) Active Directory Certificate Server.
- 7) Active Directory Federation Services (AD FS).
- 8) Active Directory Lightweight Directory Services (AD LDS).

9) Active Directory Rights Management services (AD RMS).

10) Device Health Attestation.

11) Fax Server.

12) File and Storage Services.

13) Host Guardian service.

14) Network Policy and Access Services.

15) Print and Document services.

16) Remote Access.

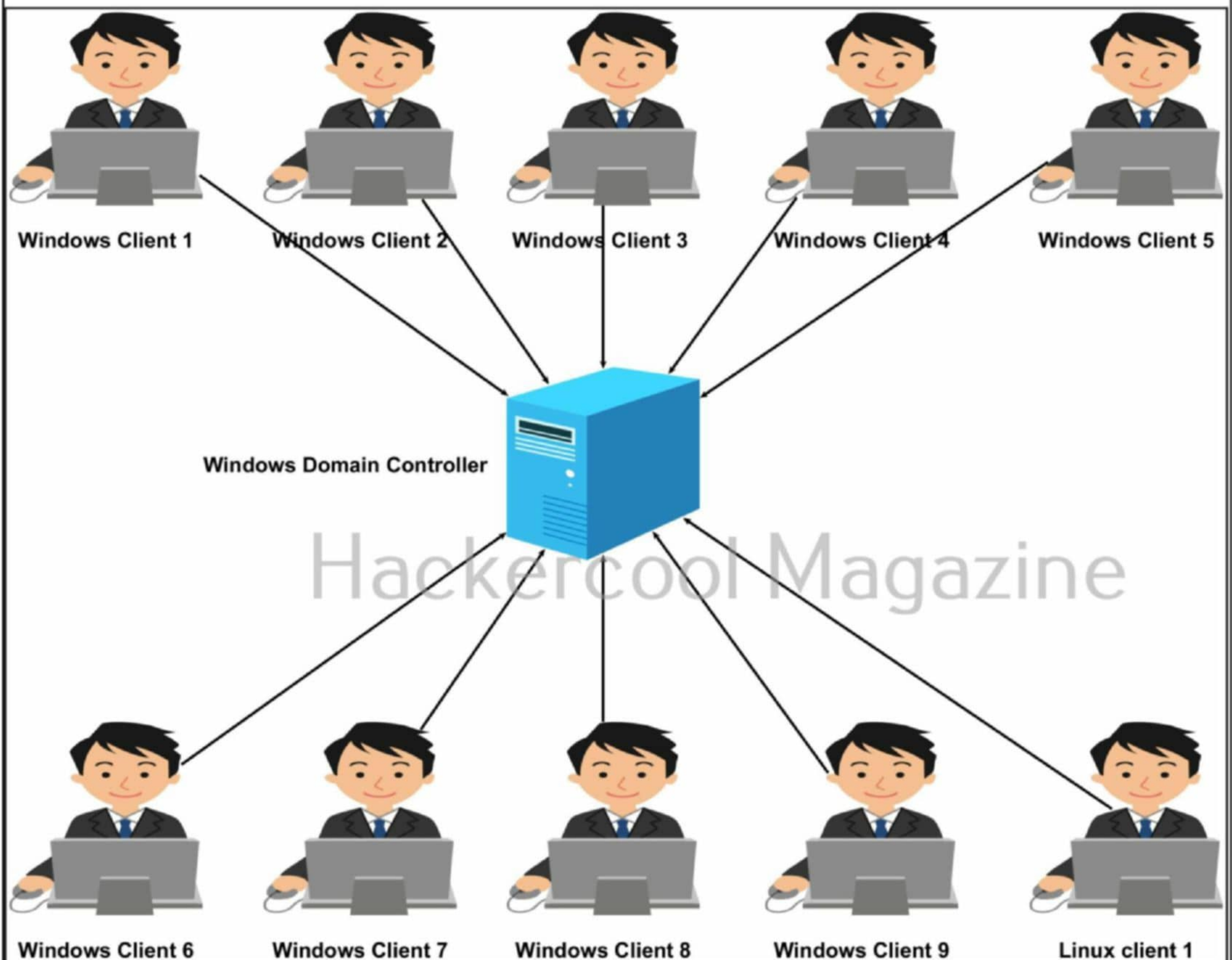
17) Remote Desktop service.

18) Volume Activation Service.

19) Windows Deployment Service

20) Windows Server updated Service

The Windows Server on which Active directory domain Services are installed is called as a Domain Controller. All other machines joining this domain are called client machines.



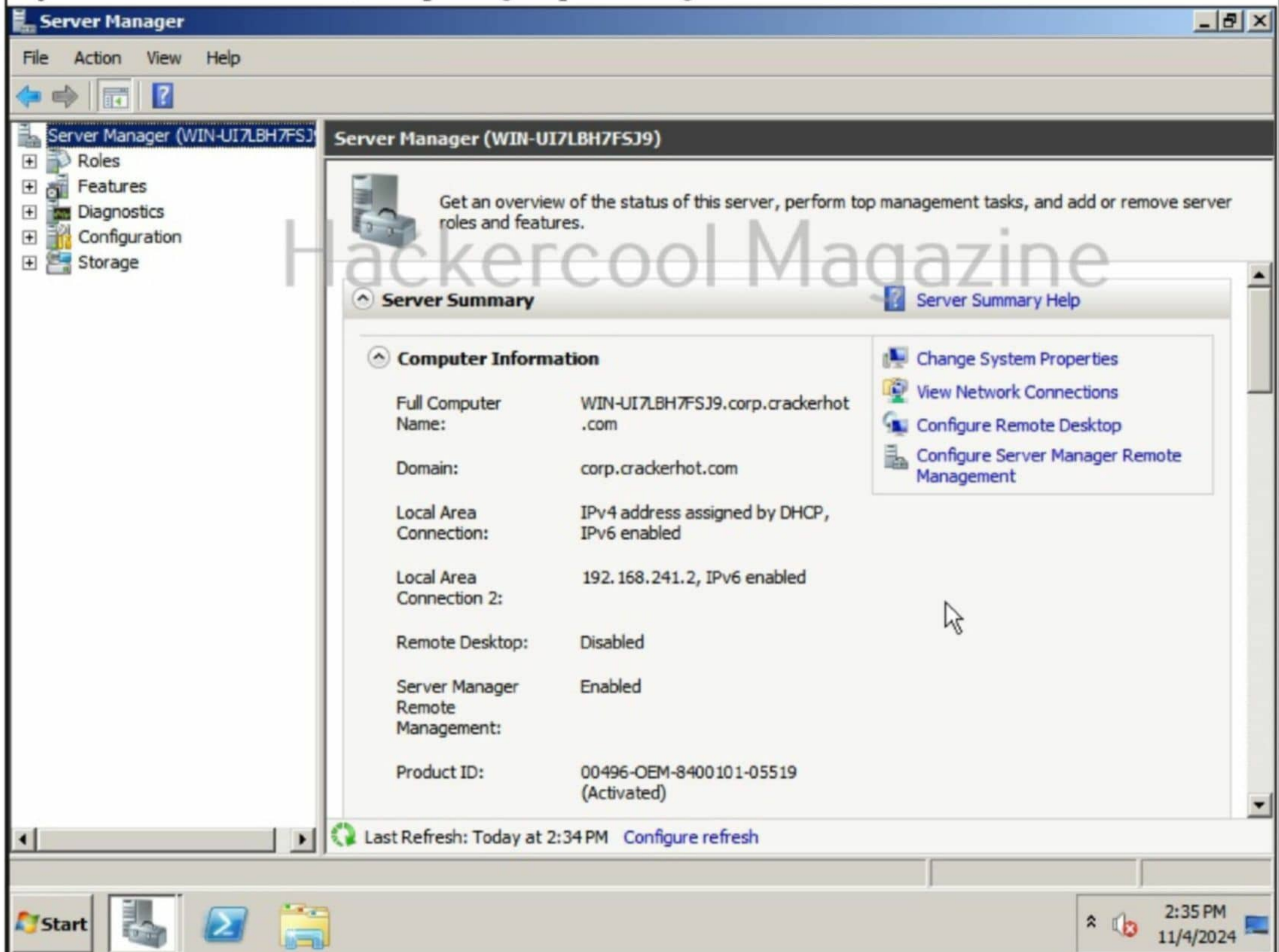
Active directory is used by over 50,410 companies globally. Majority of these are in USA. Over 80% of Fortune 1000 companies use Active Directory in their organization.

It is estimated that over 95 million Active directory accounts are attacked every day. More than 40% of these attacks are successful in real-world. Over 50% of the organization have experienced a-

n attack on Active directory in the last two years. Penetration testers successfully exploit exposed Active Directory services 82% of the time.

Before we go deep into Hacking Active Directory, you need to first understand some terms and basics of Active Directory. Mainly Active Directory has a server and client. The server has Active Directory Domain services is enabled on it. Then the workstation is said to be in a domain.

1) **Domain:** A domain commonly means a name of the website. For example, our domain is hackercoolmagazine.com. In Active Directory, a domain is a management boundary in which all the objects within it can be manageable. In simple terms, a domain is a collection of Active Directory objects which can be users, computer groups and organizational units.

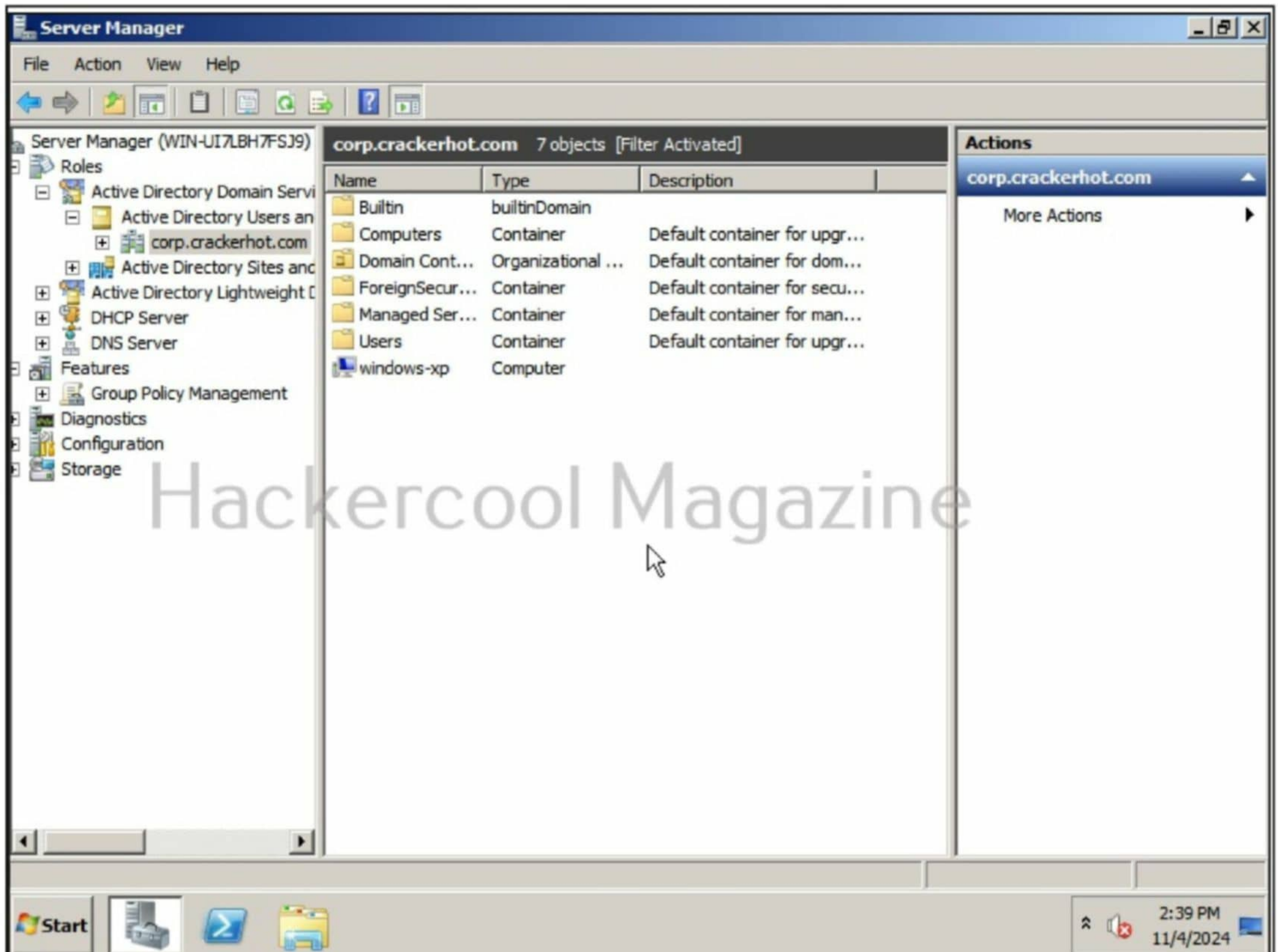


2) **Domain Controller:** A server providing Active Directory Services is called a Domain Controller. All other systems that join this domain are called as clients.

3) **Objects:** Earlier we have learnt that a domain is a collection of objects. These objects are like single units of a domain. The objects can be users, Groups, Computers, Server etc.

“The mean number of days that a hacker resides within a victim's AD network before detection is 200+ and 75% of attacks are done via compromised credentials.”

- Alex Simons, director of program management for Active Directory at Microsoft.



4) Organizational Units (OU): Another term you will often see in Active Directory, OU's are organizational units of a domain. As its name says, the organizational units can be used to group users, computers and servers into separate units. This will help to administer a policy to a specific group.

5) Forest: A collection of one or two domains is called a forest. These basics are enough for now about Active Directory.

In our upcoming Issues, you will learn more about hacking Active Directory.

According to CrowdStrike threat report 2023, there has been a 583% increase in Kerberoasting attacks in 2023.

TrendMicro Cloud Edge CVE-2024-48904

VULNERABILITY FOR BEGINNERS



Trend Micro Cloud Edge is a Unified Threat Management (UTM) device or appliance that is used to protect a network against threats by combining the physical appliance with a cloud scanning function. A vulnerability has been detected in some versions of the appliance. Trend Micro, a global cybersecurity company safeguards over 5,00,000 organizations and 250 million individuals around the world.



About the vulnerability

The vulnerability being tracked as CVE-2024-48904 is a command injection vulnerability that can lead to remote code execution. This command injection vulnerability is due to improper neutralization of special elements within commands.



No doubt, it has been assigned score of 9.8 by CVSS 3.1 rating making it a critical vulnerability. The versions affected by this vulnerability are 5.65p2 and 7.0.

“Without great security, all this great work we do around digital identity isn’t worth the electrons it is written on,”

- Alex Simons, director of program management for Active Directory at Microsoft.



**TrendMicro Cloud Edge
Unified Threat Management**



Network Gateway



Network Switch



Employee



Employee



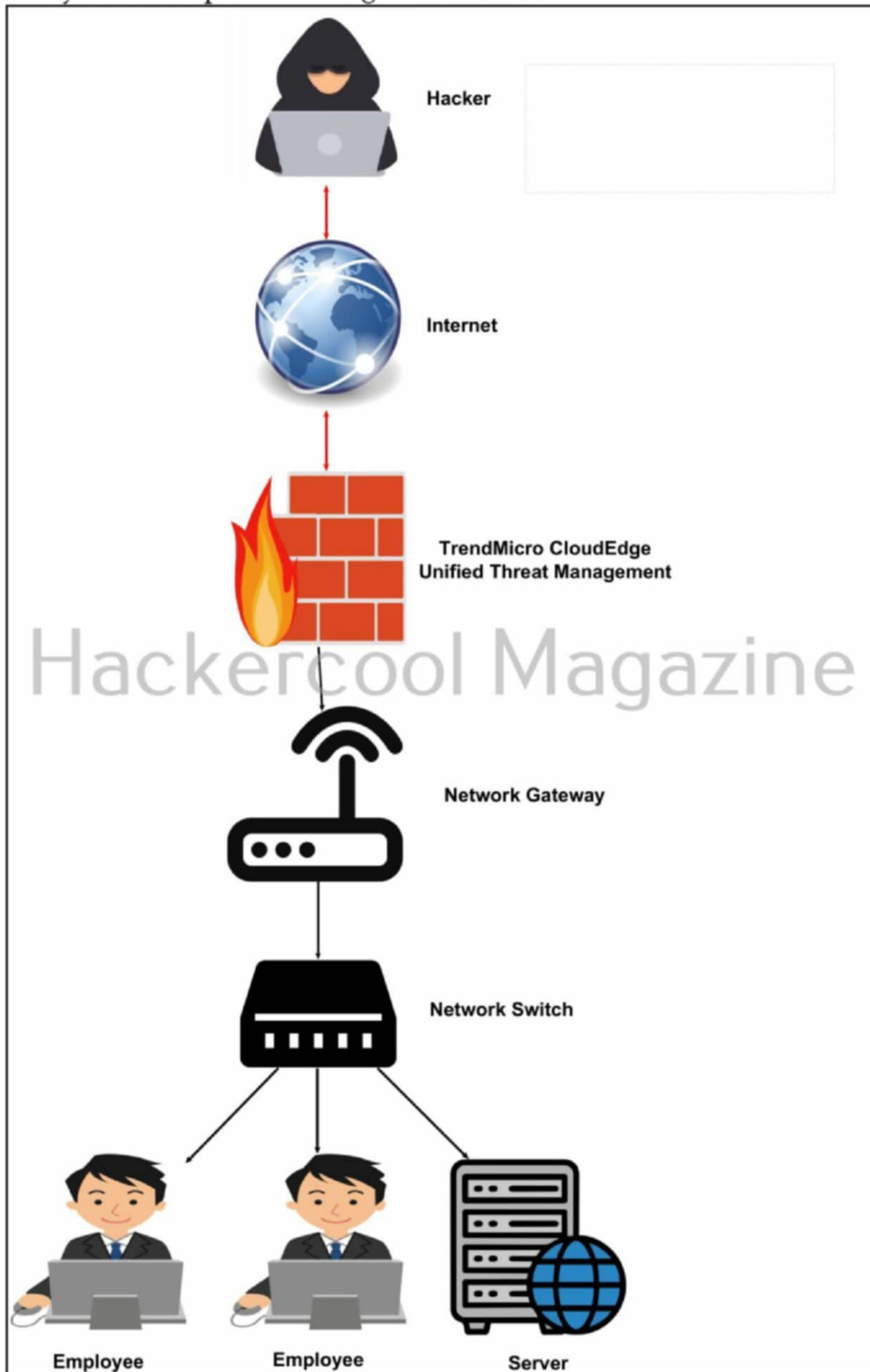
Server

Hackercool Magazine

Exploitation of this vulnerability doesn't require an authentication (Low complexity, no privileges or interaction)

How this vulnerability can be exploited?

This vulnerability can be exploited through the network.



Exploitation of this vulnerability doesn't require any authentication or for that matter even user interaction.

Impact

The simplicity with which this vulnerability can be exploited and lack of authentication or user interaction makes this vulnerability very dangerous. This vulnerability can allow hackers to execute remote code on the target appliance.

How to prevent its exploitation?

Patches have already been released for this vulnerability. Users need to upgrade to versions 5.6.3228 or 7.01081 to stay safe. Administrators also can limit network access to the UTM device to reduce exposure of the vulnerable device. Monitoring and logging of network communications should be performed to detect exploitation attempts. Firewall Intrusion Detection systems can log potentially suspicious traffic.

As an ethical hacker, i can't believe the risk people routinely take when they access the internet in public

ONLINE SECURITY

Christopher Patrick Hawkins
Lecturer in Cyber Security and Computer
Science, University of Staffordshire

In the modern world we are all constantly connected, but this comes with risks. As most cybersecurity specialists will tell you, the biggest vulnerability in any system is the user – whether at home or work.

The most common ways in which hackers break into systems are via attacks on users such as phishing, rather than by breaching technical infrastructure. As much as 94% of all malware is delivered via email, while phishing is the primary means of attack in 41% of all incidents. This risk is also increasing, with 75% of security experts reporting an overall rise in cyberattacks year on year in 2023.

Many corporate IT teams have been spending heavily on training users to be more wary of such attacks. However, this has tended to focus on best practice in the workplace. In public areas, where people's guards might be lowered, it's quite

a different story.

I've recently seen several examples of this for myself. As a certified ethical hacker with years of experience in cybersecurity and contributing to cybercriminal investigations, I can't tell you how easy it is for these kinds of situations to be exploited by bad actors.

In the first incident, I was in a shop buying some household items. While I queued, staff were asking customers for email addresses to send them e-receipts for their items.

This might sound innocent, and it's surely better for the environment than paper receipts, but it could easily be exploited by a savvy hacker who might be listening. Combined with contextual information such as location, item and cost, they could craft a phishing email that would probably fool most people. It could be an invite to complete a feedback survey, for instance, or a discount code for their next visit to the same store.

On another occasion I was at a live concert. While we waited for the show to begin, an individual in front of me was browsing his phone.

(Cont'd On Next Page)

From observing for just a short time, I ascertained his name, job, address, vehicle, phone number and even bank balance. Again, this could have been used by a hacker in a number of malicious ways, including posing as the individual to steal their identity or even coercing them to act against their employer, say by threatening to reveal sensitive information.

We therefore all need to be mindful of the information that we are exposing to strangers when we are in public. Equally, we need to think about what devices we are using, and what we are connecting them to.

Unsecured network risks

While at the same concert, I saw numerous people connecting to the stadium wifi, which was totally unprotected and required no authentication. When you log in to an unsecured network, it exposes your device to risks such as evil twin attacks.

Evil twin attacks involve the attacker creating a wifi hotspot, which can be set to any name they choose, such as "stadium wifi 2" or whatever. When an unprotected device connects to this network, the attacker can potentially steal the data they are transmitting.

It can also be used for other nefarious purposes such as snooping on confidential networks, injecting malware into downloads or "man-in-the-middle" attacks in which the hacker poses as the other person in a communication, again usually to

steal information.

People can be exposed to similar threats on unsecured networks through another hacking ruse known as packet sniffing. This is where a hacker uses a program to monitor the data moving over the network and steal information.

You can avoid these risks by logging in from a virtual private network (VPN), not that I saw anyone doing that at the concert. More generally, people can protect themselves from identity theft by, for instance, having anti-phishing systems in their inboxes.

However, the easiest defence of all is to be

"The easiest defence of all is to be alert to the risks and take sensible precautions in public. By protecting your data and devices, no matter where you are, you can avoid becoming one of the victims."

alert to the risks and take sensible precautions in public. By protecting your data and devices, no matter where you are, you can avoid becoming one of the victims.

**This
Article
first
appeared
in
The
Conversation**

Converting Python scripts to binaries

EXPLOIT WRITING

One of the readers of our Magazine has recently asked me a question. The question comes something like this. It's all good creating exploit scripts and payloads (or something like that) with python but what about sharing these scripts or payloads to target users to be executed by them.

The meaning of his question he wanted to ask is something like this. If we write an exploit or payload and want our target users to execute it on their systems, how should we do this.

It is a very good question indeed. If we want our target user to execute our payloads or scripts written in Python, he should have Python installed on this system. Although this could be a good beginning of an execution chain, it would be good and more successful if it can be executed directly on the target system without the need of Python.

The best way to make it possible is to convert the script into a binary (Windows executable for Windows and bash script for Linux targets). If we convert it to a Windows executable it could be executed on multiple Windows operating systems, no matter Python is installed or not. The same is true with Linux binaries. In this article, let's see one method of doing it. But first, let's create a simple Python script named "hc.py" with code shown below.

Message="Hello World"

Print(Message)

```
GNU nano 7.2 hc.py
message = "Hello World";
print(message)
```

[Read 2 lines]

^G Help ^O Write Out ^W Where Is ^K Cut
^X Exit ^R Read File ^\ Replace ^U Paste

You know what this script does. When we execute it, it prints us a "Hello World" message as shown below.

```
(kali㉿kali)-[~/Desktop]
$ python3 hc.py
Hello World
```

I have written this code on Kali Linux. Now, let's move it to a Windows machine and execute it to see if we get the same result (Of course, Python should be installed on Windows).

"More routine initial exploitation of zero-day vulnerabilities represents the new normal which should concern end-user organizations and vendors alike as malicious actors seek to infiltrate networks." - Ollie Whitehouse, NCSC's chief technology officer.


```
C:\Users\ADMIN>hc.py
```

```
C:\Users\ADMIN>python hc.py
```

```
Hello World
```

```
C:\Users\ADMIN>
```

The result is same. Now, let's turn this into a Windows executable. We have to do this on the Windows system.

For this purpose, we will use a tool called PyInstaller. PyInstaller is used to package Python code into stand alone executables for various operating systems. It can be installed using pip as shown below.

```
C:\Users\ADMIN>pip install pyinstaller
```

```
Defaulting to user installation because normal site-packages is not writeable
```

```
Collecting pyinstaller
```

```
  Downloading pyinstaller-6.11.0-py3-none-win_amd64.whl.metadata (8.4 kB)
```

```
Collecting setuptools>=42.0.0 (from pyinstaller)
```

```
  Downloading setuptools-75.3.0-py3-none-any.whl.metadata (6.9 kB)
```

```
Collecting altgraph (from pyinstaller)
```

```
  Downloading altgraph-0.17.4-py2.py3-none-any.whl.metadata (7.3 kB)
```

```
Collecting pyinstaller-hooks-contrib>=2024.8 (from pyinstaller)
```

```
  Downloading pyinstaller_hooks_contrib-2024.9-py3-none-any.whl.metadata (16 kB)
```

```
Collecting packaging>=22.0 (from pyinstaller)
```

```
  Downloading packaging-24.1-py3-none-any.whl.metadata (3.2 kB)
```

```
Collecting pefile!=2024.8.26,>=2022.5.30 (from pyinstaller)
```

```
  Downloading pefile-2023.2.7-py3-none-any.whl.metadata (1.4 kB)
```

```
Collecting pywin32-ctypes>=0.2.1 (from pyinstaller)
```

```
  Downloading pywin32_ctypes-0.2.3-py3-none-any.whl.metadata (3.9 kB)
```

```
Downloading pyinstaller-6.11.0-py3-none-win_amd64.whl (1.3 MB)
```

```
----- 1.3/1.3 MB 4.9 MB/s eta 0:00:00
```

```
Downloading packaging-24.1-py3-none-any.whl (53 kB)
```

```
Downloading pefile-2023.2.7-py3-none-any.whl (71 kB)
```

```
Downloading pyinstaller_hooks_contrib-2024.9-py3-none-any.whl (336 kB)
```

```
Downloading pywin32_ctypes-0.2.3-py3-none-any.whl (30 kB)
```

```
Downloading setuptools-75.3.0-py3-none-any.whl (1.3 MB)
```

```
----- 1.3/1.3 MB 4.5 MB/s eta 0:00:00
```

```
Downloading altgraph-0.17.4-py2.py3-none-any.whl (21 kB)
```

If that doesn't work, use this command below.

In 2023, CrowdStrike observed a 60% year-over-year increase in the number of interactive hacking campaigns, with a 73% increase in the second half compared to 2022.


```
C:\Users\ADMIN>pip install -U pyinstaller
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pyinstaller in c:\users\admin\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (6.11.0)
Requirement already satisfied: setuptools>=42.0.0 in c:\users\admin\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from pyinstaller) (75.3.0)
Requirement already satisfied: altgraph in c:\users\admin\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from pyinstaller) (0.17.4)
Requirement already satisfied: pyinstaller-hooks-contrib>=2024.8 in c:\users\admin\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from pyinstaller) (2024.9)
Requirement already satisfied: packaging>=22.0 in c:\users\admin\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from pyinstaller) (24.1)
Requirement already satisfied: pefile!=2024.8.26,>=2022.5.30 in c:\users\admin\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from pyinstaller) (2023.2.7)
```

Once installed, all you have to do is run command shown below.

python -m PyInstaller <Python exploit script>

It is shown below.

```
C:\Users\ADMIN>python -m PyInstaller hc.py
633 INFO: PyInstaller: 6.11.0, contrib hooks: 2024.9
634 INFO: Python: 3.12.7
656 INFO: Platform: Windows-10-10.0.19045-SP0
656 INFO: Python environment: C:\Program Files\WindowsApps\PythonSoftwareFoundation.Python.3.12_3.12.2032.0_x64__qbz5n2kfra8p0
658 INFO: wrote C:\Users\ADMIN\hc.spec
667 INFO: Module search paths (PYTHONPATH):
['C:\\Users\\ADMIN',
 'C:\\Program '
 'Files\\WindowsApps\\PythonSoftwareFoundation.Python.3.12_3.12.2032.0_x64__qbz5n2kfra8p0\\python312.zip',
 'C:\\Program '
 'Files\\WindowsApps\\PythonSoftwareFoundation.Python.3.12_3.12.2032.0_x64__qbz5n2kfra8p0\\DLLs',
 'C:\\Program '
 'Files\\WindowsApps\\PythonSoftwareFoundation.Python.3.12_3.12.2032.0_x64__qbz5n2kfra8p0\\Lib',
 'C:\\Program '
 'Files\\WindowsApps\\PythonSoftwareFoundation.Python.3.12_3.12.2032.0_x64__qbz5n2kfra8p0',
 'C:\\Users\\ADMIN\\AppData\\Local\\Packages\\PythonSoftwareFoundation.Python.3.12_qbz5n2kfra8p0\\LocalCache\\local-packages\\Python312\\site-packages',
 'C:\\Program '
 'Files\\WindowsApps\\PythonSoftwareFoundation.Python.3.12_3.12.2032.0_x64__qbz5n2kfra8p0\\Lib\\site-packages',
```

Over 500 million Active Directory users exist and over 95 million of these users are attacked every day.




```

10710 INFO: Building PYZ (ZlibArchive) C:\Users\ADMIN\build\hc\PYZ-00.pyz completed successfully.
10732 INFO: checking PKG
10732 INFO: Building PKG because PKG-00.toc is non existent
10734 INFO: Building PKG (CArchive) hc.pkg
10769 INFO: Building PKG (CArchive) hc.pkg completed successfully.
10770 INFO: Bootloader C:\Users\ADMIN\AppData\Local\Packages\PythonSoftwareFoundation.Python.3.12_qbz5n2kfra8p0\LocalCache\local-packages\Python312\site-packages\PyInstaller\bootloader\Windows-64bit-intel\run.exe
10770 INFO: checking EXE
10773 INFO: Building EXE because EXE-00.toc is non existent
10773 INFO: Building EXE from EXE-00.toc
10774 INFO: Copying bootloader EXE to C:\Users\ADMIN\build\hc\hc.exe
10828 INFO: Copying icon to EXE
10835 INFO: Copying 0 resources to EXE
10835 INFO: Embedding manifest in EXE
10841 INFO: Appending PKG archive to EXE
10843 INFO: Fixing EXE headers
11050 INFO: Building EXE from EXE-00.toc completed successfully.
11051 INFO: checking COLLECT
11051 INFO: Building COLLECT because COLLECT-00.toc is non existent
11053 INFO: Building COLLECT COLLECT-00.toc
11174 INFO: Building COLLECT COLLECT-00.toc completed successfully.

C:\Users\ADMIN>_

```

This will create a new directory (folder in Windows) named “dist” as shown below.

```

01/24/2023  06:10 PM    <DIR>          .ms-ad
09/09/2024  02:02 PM    <DIR>          .VirtualBox
01/03/2024  03:30 PM    1,665 2.ps1
06/24/2024  04:30 PM    <DIR>          3D Objects
11/07/2024  11:27 AM    <DIR>          build
01/14/2023  08:46 AM    <DIR>          Contacts
11/07/2024  10:53 AM    <DIR>          Desktop
11/07/2024  11:27 AM    <DIR>          dist
09/30/2023  12:56 PM                259,214 Document-1-page001.png

```

Inside this directory, our compiled Windows executable will be located.

“The average cost to a company due to data breach is \$3.5 million”.

- Alex Simons, director of program management for Active Directory at Microsoft.


```

C:\Users\ADMIN>dir dist
Volume in drive C has no label.
Volume Serial Number is F87C-3955

Directory of C:\Users\ADMIN\dist

11/07/2024  11:27 AM    <DIR>          .
11/07/2024  11:27 AM    <DIR>          ..
11/07/2024  11:27 AM    <DIR>          hc
               0 File(s)                0 bytes
               3 Dir(s)  19,785,433,088 bytes free

```

```
C:\Users\ADMIN>cd _
```

```
C:\Users\ADMIN\dist>cd hc
```

```

C:\Users\ADMIN\dist\hc>dir
Volume in drive C has no label.
Volume Serial Number is F87C-3955

Directory of C:\Users\ADMIN\dist\hc

11/07/2024  11:27 AM    <DIR>          .
11/07/2024  11:27 AM    <DIR>          ..
11/07/2024  11:27 AM             1,626,334 hc.exe
11/07/2024  11:27 AM    <DIR>          _internal
               1 File(s)            1,626,334 bytes
               3 Dir(s)  19,788,898,304 bytes free

```

```
C:\Users\ADMIN\dist\hc>_
```

Let's execute this binary and see if its functionality is same.

Name	Date modified	Type	Size
 _internal	11/7/2024 11:27 AM	File folder	
 hc.exe	11/7/2024 11:27 AM	Application	1,589 KB

```

C:\Users\ADMIN\dist\hc>hc.exe
Hello World

```

```
C:\Users\ADMIN\dist\hc>_
```

As you can see, its working successfully,

Hacking attacks targeting Cloud based networks increased by over 110% in 2023 compared to 2022, according to CrowdStrike

DOWNLOADS

[Parrot OS 6.2](#)

<https://parrotsec.org/download/>

USEFUL RESOURCES

[Check whether your email is a part of any data breach](#)

<https://haveibeenpwned.com>

[Vulnera](#)

<https://github.com/hackercoolmagz/vulnera>

Follow Hackercool Magazine for latest updates



Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2019
Bundle**

Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2020
Bundle**

Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2021
Bundle**

Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2022
Bundle**

Buy now